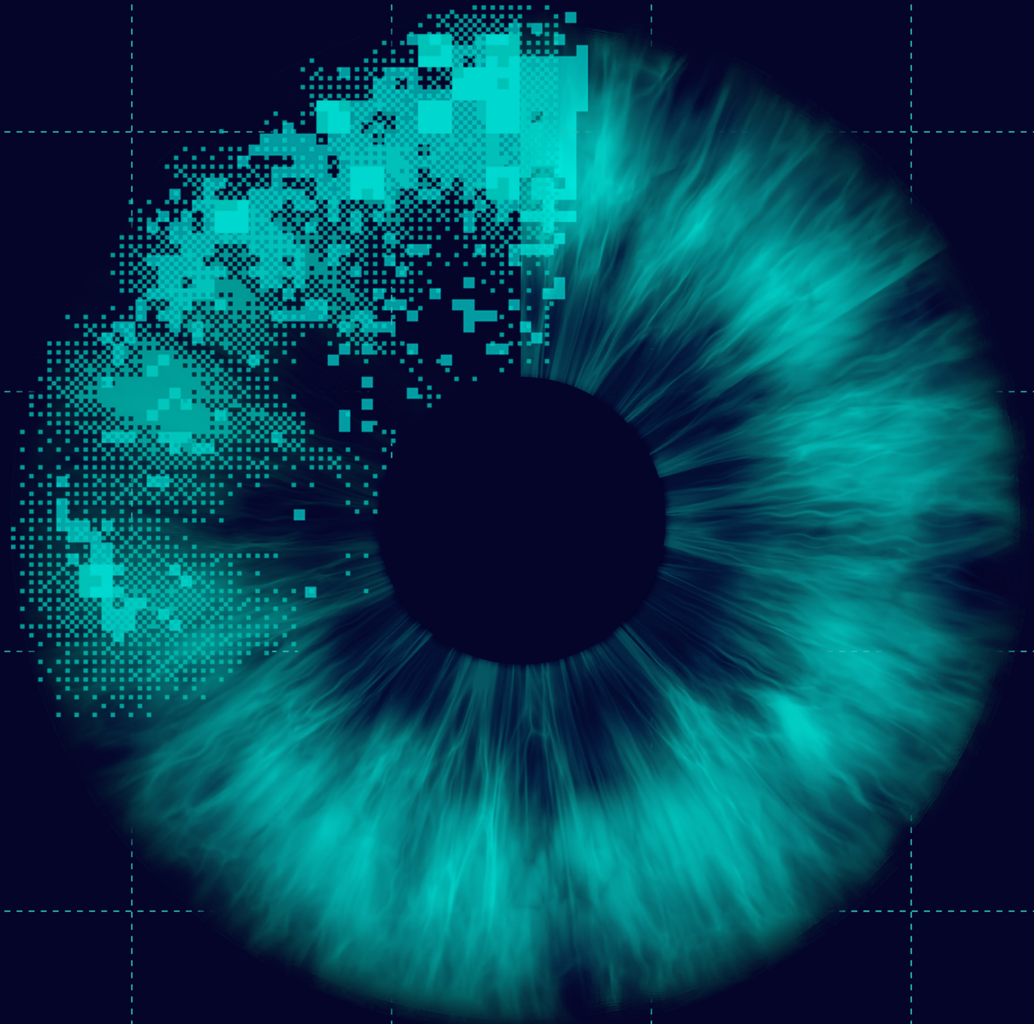


SEON

The Next Layer of Defense

How Leading Retailers Extend Their Fraud Controls

Insights from SEON's 2026 Fraud & AML Leaders Survey

Table of Contents

Executive Summary & Methodology

Executive Summary

Retailers have never had more tools to accelerate online growth. Today's eCommerce platforms make it remarkably easy to launch storefronts, scale globally and process massive transaction volumes. But when it comes to fraud prevention, this exact convenience has created a hidden, systemic vulnerability.

Currently, 62% of retail organizations rely entirely or mostly on the rudimentary fraud protections built directly into their eCommerce platforms. On the surface, the appeal is obvious. Platform-native tools promise speed and simplicity — offering built-in rules, automated risk checks and seamless payment integrations that let retailers deploy fast without wrestling with complex risk infrastructure.

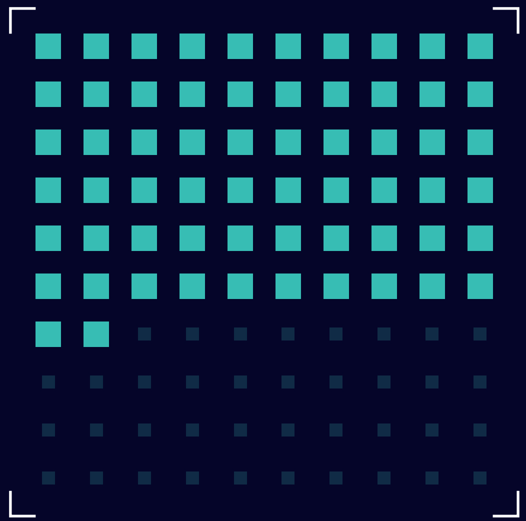
Yet, the data reveals a striking contradiction. Among the retailers relying primarily on these built-in controls, nearly half report that their fraud losses are growing faster than their revenue. Simply put, the tools retailers depend on most are failing to keep pace with the threats they face.

This is not a technology problem. It is a coverage problem. Platform-native fraud controls were designed to facilitate commerce, not to defend against sophisticated, AI-backed fraud ecosystems. As online retail expands and financial crime becomes increasingly automated, the gap between perceived protection and actual exposure continues to widen.

This report traces that widening gap across three dimensions: the expanding attack surface driven by rapid retail growth, the critical shift of severe fraud to pre-checkout stages and the paradox of expanding fraud teams despite near-universal AI adoption.

Reliance on Built-in Protection

How much does your organization rely on your e-commerce platform (e.g., Shopify, BigCommerce) to handle fraud prevention?



62% mostly or completely rely on their ecommerce platform's native tools for fraud prevention

Methodology

As part of SEON's **AI Reality Check: 2026 Fraud & AML Leaders Report**, this research draws on responses from 330 global retail fraud and AML leaders. It examines a structural mismatch at the heart of retail's fraud challenge: why retailers depend on platforms built for commerce rather than defense, how the most damaging fraud types begin long before checkout and why near-universal AI adoption has actually increased the demand for fraud talent. The insights are specific to the retail sector and grounded in current decision-making frameworks.

Respondents hold senior decision-making roles, including Director of Digital / Ecommerce Operations, Head of Fraud, VP of Risk, Chief Compliance Officer and equivalent C-suite titles. All data cited in this report is sourced directly from survey responses unless otherwise noted.

Key Findings

1

The Platforms Retailers Rely on Most Are Not Keeping Up

Retail fraud controls are heavily concentrated in eCommerce platform-native tools — and those tools have a hard structural ceiling. They were built to streamline commerce, not to deliver comprehensive defense. While 62% of retailers lean primarily on these built-in controls, nearly half of that group reports fraud losses outpacing revenue growth. Convenience and coverage are not the same thing, and the gap between them is costing retailers heavily.

2

Fraud Starts Before Checkout — But Controls Are Focused at the Register

The most damaging retail fraud types — account takeover, promotion abuse, return fraud and loyalty fraud — do not originate at the point of payment. They begin much earlier, hiding within account activity, login behaviors and promotion usage. Platform-native tools focus almost exclusively on transaction-level signals at checkout, meaning they are looking in the wrong place. Retailers unable to detect fraud earlier in the customer journey are trapped in a cycle of constantly playing catch-up.

3

Automation Is Expanding the Work, Not Replacing It

An overwhelming 97% of retail organizations have already implemented AI in their fraud workflows, and confidence in these tools remains high. Yet, 97% also plan to increase their fraud headcount, with nearly 60% preparing to add three or more full-time risk professionals. Why? Because AI surfaces more signals, generates more investigations and demands more governance than manual processes ever did. Automation isn’t reducing the workload; it’s expanding it. The retailers poised to win are those pairing AI with the right talent to act on what it finds.

Section 1

The Growth Paradox

More Growth, More Exposure

Retail's digital expansion shows absolutely no signs of slowing. Nearly 88% of retailers report revenue growth of 10% or more over the past 12 months, reflecting immense, sustained momentum. With new storefronts, expanding markets, and diverse payment methods, the infrastructure of modern retail is purpose-built to scale fast.

But scale cuts both ways. Unlike the financial sector, which operates with highly centralized risk teams, fraud responsibility in retail is rarely concentrated in a single place. Instead, it spans eCommerce, payments, customer operations and finance. These departments often rely on different systems, juggle conflicting priorities and operate with incomplete visibility. Coordination becomes incredibly difficult when data remains siloed, and the relentless pace of retail leaves little room for the deliberate, cross-functional risk management required actually to stop fraud.

The result is a high-growth environment that exposes organizations to fraud much faster than they are structured to handle it. Retailers operate under intense pressure to maintain a frictionless customer experience. Adding friction to the checkout flow quickly translates into abandoned carts and lost revenue. This creates a precarious balancing act: strengthening defenses without harming conversion. Fraudsters know this tension exists, and they are more than willing to exploit it.

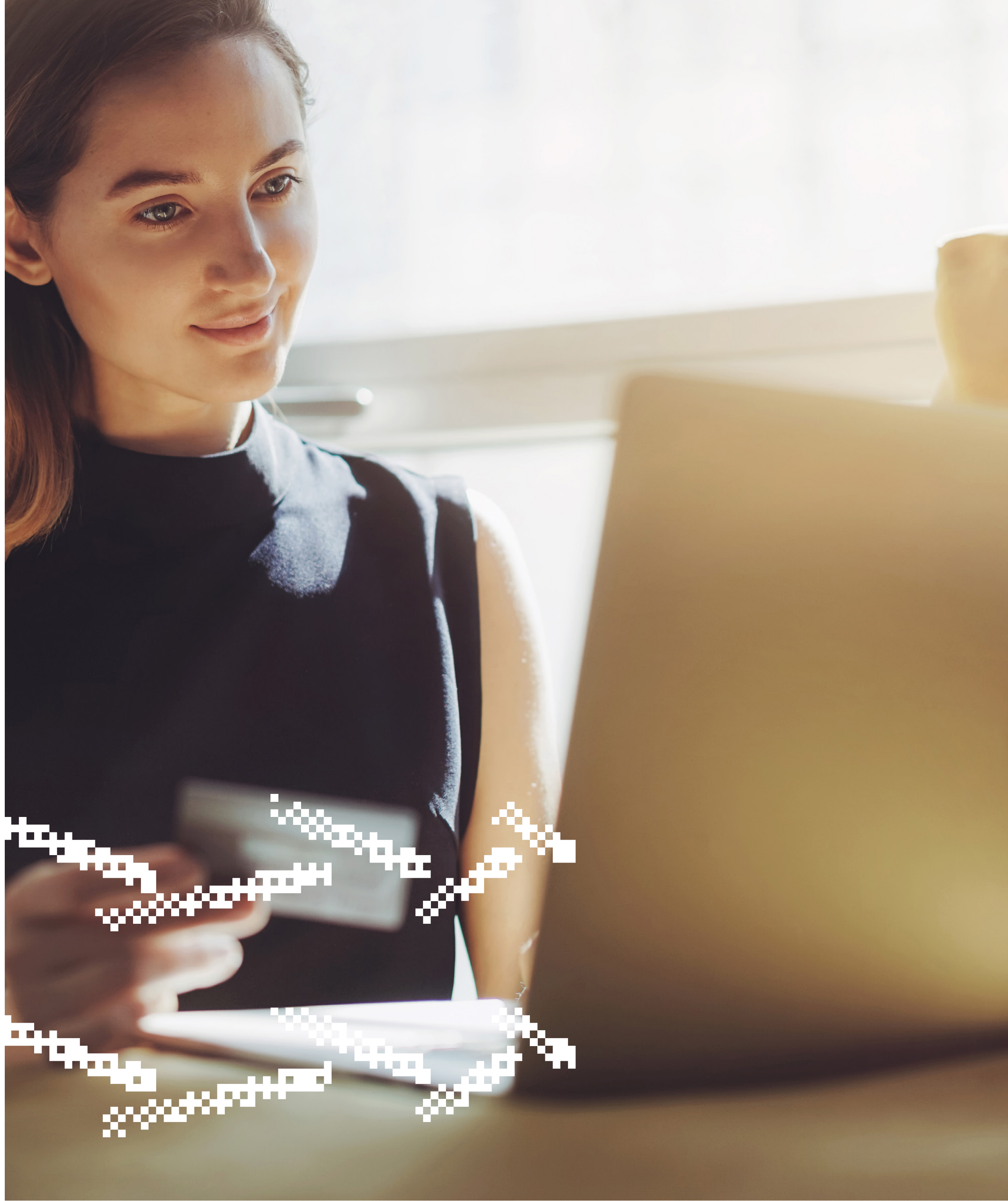
Section 2

The Detection Gap

Looking in the Wrong Place

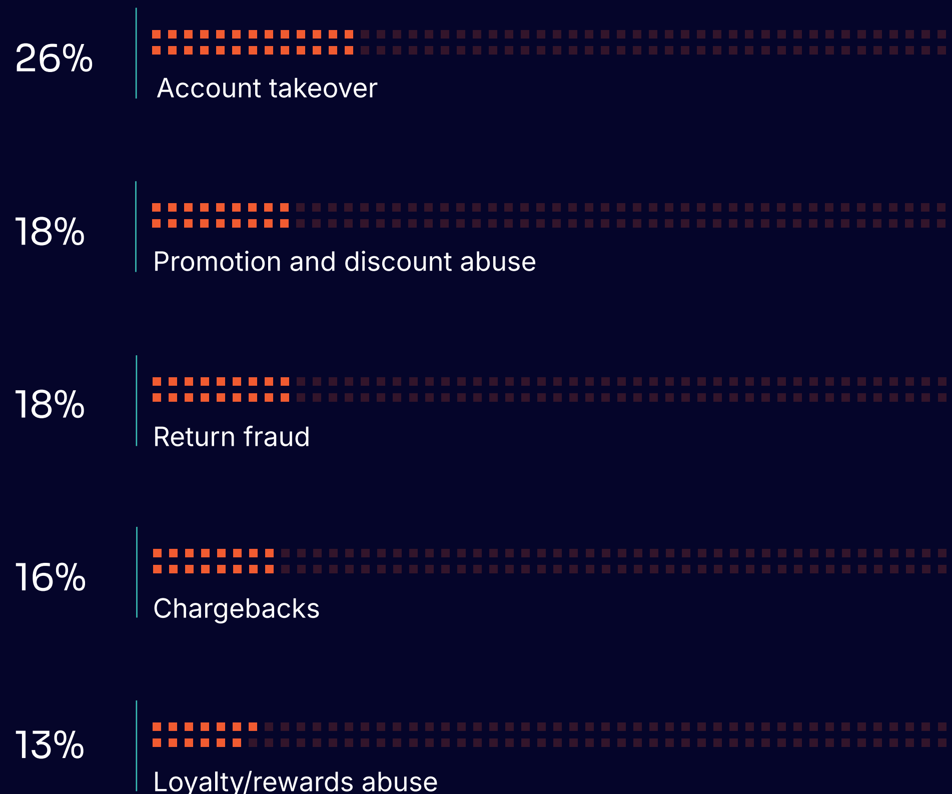
Most retail fraud strategies are built around a single, decisive moment: the transaction. Payment-level controls catch bad actors at checkout. Chargeback rules claw back disputed revenue after the fact. Platform-native risk engines score individual orders in real time.

What they fail to do is look upstream. And unfortunately, that is exactly where modern retail fraud begins.
When asked to identify their leading sources of fraud loss, respondents pointed to account takeover (26%), promotion and discount abuse (18%), return fraud (18%), chargebacks (16%) and loyalty/rewards abuse (13%).



Leading Sources of Fraud Loss

What are the primary drivers of fraud losses on your platform?



Look at that list carefully. Four of the top five fraud types originate long before the checkout event. Account takeovers start when fraudsters hijack legitimate customer profiles — often weeks before those accounts are weaponized for fraudulent purchases. Promotion abuse happens when attackers exploit new-customer incentives, spinning up synthetic identities to drain marketing budgets at scale. Loyalty fraud quietly targets the stored value inside customer accounts. By the time any of these attacks surface as a disputed transaction or a chargeback, the underlying compromise is already complete.

Platform-native tools are not designed to see this pre-checkout activity. Optimized to assess risk at the exact point of payment, they have virtually no visibility into account-level behavior, login anomalies or cross-channel identity signals. Consequently, the earliest and most actionable indicators of fraud fall completely outside their field of view.

This is the detection gap. For retailers relying solely on built-in tools, it means that fraud — which could have easily been stopped at the account level — routinely survives all the way to the transaction, and often beyond.

Section 3

The AI Dividend Problem

More AI, More Work

By almost any measure, the retail sector has fully embraced AI for fraud prevention. Today, 97% of retail organizations use AI in their fraud or AML workflows, and 95% of leaders are confident that AI can reliably detect and prevent threats. These are not tentative early adopters. Retail has moved past the question of whether to use AI and is now grappling with the much harder question of how to use it well.

Yet, despite this automation, the fraud function isn't shrinking. It's expanding. An astounding 97% of retail organizations plan to increase their fraud or AML headcount in the coming year, with nearly 60% expecting to add three or more full-time hires. In an industry that has almost universally adopted automation, this level of hiring intent demands an explanation.

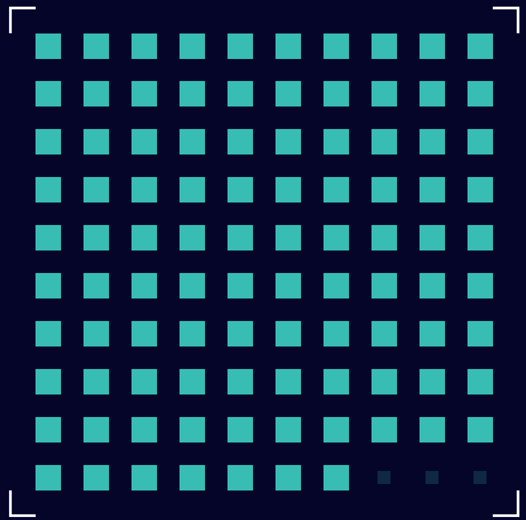
The answer lies in what AI actually does when it works. Effective AI does not reduce the volume of human decisions; it changes their nature. Automation allows teams to sift through massive data volumes and spot subtle patterns that manual reviews would never catch. But those signals generate investigations. Investigations require judgment. And judgment requires people.

As AI surfaces more suspicious activity across the entire customer lifecycle — flagging account anomalies, behavioral outliers and cross-channel identity patterns — the demand for skilled analysts who can interpret and govern those outputs skyrockets. Automation expands the frontier of what fraud teams can see, but it does not eliminate the need for human experts to act on those insights.

The retailers that extract the most value from their AI investments this year will be those that treat automation as a capability multiplier, rather than a headcount substitute.

Plans to Increase Fraud and AML Headcount

Are you planning to expand your fraud and AML team this year?



97% of retail organizations plan to increase their fraud or AML headcount

Section 4

The Pre-Built Platform Ceiling

Retail's fraud challenge is not a technology problem. The tools exist. AI adoption is near-total. Platforms are more capable than ever. The true challenge is a coverage problem — a fundamental structural mismatch between where fraud controls are focused and where fraud actually occurs.

Platform-native tools were built to move commerce forward, and they do that exceptionally well. But they were never designed to detect the coordinated, multi-stage fraud that spans account creation, identity manipulation and promotion exploitation. Retailers relying on them as a complete solution are, by definition, operating with massive blind spots.

Closing this gap means expanding the frame. It requires moving fraud detection earlier in the customer journey — shifting the focus from checkout back to account creation, login behavior and promotion use. It means connecting signals across disparate systems that were never designed to share data. Above all, it means treating AI not as a replacement for human judgment, but as the critical infrastructure that enables that judgment to be faster, sharper and far more scalable.

Before rushing to add another point solution, every retail fraud leader should evaluate their foundational readiness by asking three key questions:

Before rushing to add another point solution, every retail fraud leader should evaluate their foundational readiness by asking three key questions:

→ **Are our fraud controls covering the full customer journey — or just the checkout?**

If your primary defenses sit entirely within your eCommerce platform, you are almost certainly missing the earliest, most actionable signals. Account takeover, promotion abuse and loyalty fraud all begin upstream. If your detection starts at the transaction, you are already too late.

→ **Are we measuring the right thing?**

Chargeback and transaction decline rates are standard metrics, but they measure outcomes rather than exposure. Do you have true visibility into account-level anomalies, promotion usage patterns and the behavioral signals that precede a fraudulent transaction? If not, your picture of risk is fundamentally incomplete.

→ **Is our AI investment building a long-term capability — or just adding another point solution?**

With 97% of retailers adopting AI in some form, the question isn't whether you have it, but whether it has access to the right data. AI built on fragmented, transaction-only data will only ever surface transaction-level insights. AI built on a unified view of the entire customer lifecycle will surface the fraud that is actually costing you money.

Get the Full Picture

This report covers the retail-specific findings from 330 fraud and AML leaders worldwide. For the complete analysis — AI adoption benchmarks, vendor ecosystem trends, investment forecasts and the full dataset from 1,010 respondents across betting and gaming, fintech, payments and retail — download the full report.

⟶ **Download the AI Reality Check: 2026 Fraud & AML Leaders Report**

⟶ **Talk to a SEON Expert**

Based on SEON's 2026 Fraud & AML Leaders Survey. 1,010 respondents across betting and gaming, fintech, payments and retail. Research conducted by Jane Singh & Katy Chrisler. IDV data sourced from SEON's 2026 IDV Market Research (85 betting and gaming operators).

SEON

The Command Center for Fraud Prevention & AML Compliance

This report is based on insights from a survey commissioned by SEON, gathering perspectives from fraud prevention and compliance professionals across industries. Research and analysis were conducted by Jane Singh & Katy Chrisler.

Read more at seon.io

The Total Opportunity Cost of Fraud is Bigger Than You Think

Read Article ⟶

Leveraging AI & Innovative Tech to Combat Emerging Complex Fraud Schemes

Read Article ⟶

Traditional Fraud Prevention Measures Aren't Enough

Read Article ⟶